UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

OTR TRANSPORTATION, INC., an Illinois Corporation,	)	
Plaintiff,	)	COMPLAINT
v.	)	
	)	Civil Action No. 1:21-cv-3415
DATA INTERFUSE, LLC, a Virginia Limited liability company, and JOHN LOVEGROVE, an individual,	)	
	)	JURY DEMAND
Defendants.	)	

COMPLAINT

Plaintiff OTR TRANSPORTATION, INC. by and through its attorneys Thomas P. Yardley and Christine R. Walsh of Robbins, Salomon & Patt, Ltd., for its Complaint against DATA INTERFUSE, LLC and JOHN LOVEGROVE, states as follows:

NATURE OF ACTION

1. This is an action for violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA"); the Illinois Trade Secret Act, 765 ILCS 1065, the Defend Trade Secrets Act ("DTSA"), 18 U.S.C.A. § 1839; and intentional interference with contractual relations, all arising from conduct engaged in by the Defendants Data Interfuse, Inc. ("DI") and John Lovegrove ("Lovegrove") that caused harm to the Plaintiff OTR Transportation Inc. ("OTR").

2. By this action, OTR seeks statutory damages, compensatory damages, punitive damages, attorney's fees and costs, injunctive relief, and all other relief to which they may be entitled and as deemed appropriate by this Court.

PARTIES

3. OTR is an Illinois corporation with its principal place of business in Chicago, Illinois.

4. OTR is in the business of brokering freight and providing other logistical services to its customers. OTR provides freight brokerage and logistic services to customers by connecting carriers with shippers and consigners to transport goods throughout the United States.

5. DI is a Virginia limited liability company with a principal place of business in Fairfax County, Virginia.

6. Upon information and belief, the members of DI are citizens of the Commonwealth of Virginia and are not citizens of the state of Illinois.

7. DI is in the business of business analysis and data infrastructure consulting.

8. Lovegrove is an employee of DI. Upon information and belief, Lovegrove is a citizen of the state of Virginia.

JURISDICTION AND VENUE

9. This Court has jurisdiction over the subject matter of the Plaintiff's federal statutory claims pursuant to 28 U.S.C. § 1331. This Court has supplemental jurisdiction over the subject matter of the Plaintiff's state law claims pursuant to 28 U.S.C. § 1367. The Court also has diversity jurisdiction over the Plaintiff's state law claims pursuant to 28 U.S.C. § 1332(a) because the parties are citizens of different states and the amount in controversy is in excess of $75,000, exclusive of interest and costs based upon the damages caused to OTR's data systems and business and the payment of fees and costs incurred investigating DI and Lovegrove's misconduct.

10. This Court may exercise personal jurisdiction over DI because DI routinely does business in Illinois, and this lawsuit arises out of DI's unlawful access of OTR's data and computer

systems, which are owned by OTR, an Illinois corporation, and the resulting harm which defendants caused OTR in Illinois.

11. This Court may exercise personal jurisdiction over Lovegrove because Lovegrove routinely works for Illinois customers, and Lovegrove routinely worked with and communicated with OTR in Illinois. Lovegrove traveled to Illinois while servicing OTR's account with DI, and this lawsuit arises out of Lovegrove's intentional conduct that involved unlawfully accessing OTR's data and computer systems, which were based in Illinois, and caused harm to OTR in Illinois.

12. The Defendants engaged in intentional conduct with actual malice that has harmed the Plaintiff.

13. The Plaintiff has been injured by the Defendants' conduct and have suffered damages well in excess of $75,000 resulting therefrom.

FACTUAL BACKGROUND

14. In connection with its freight brokerage business, OTR desired to develop a proprietary pricing model to determine, at a granular, specific, and targeted level, price fluctuations in shipment and carrier costs across the country to gain a competitive advantage in pricing for its customers and prospective customers.

15. OTR developed a proprietary software system and required the services of IT support and software development in order to expand upon and improve OTR's proprietary software systems to use in its business.

16. During the fall of 2018, DI solicited OTR to provide IT support and software development services, including, but not limited to, software development, coding, and

engineering services for OTR to use in its freight brokerage business to assist OTR in developing and improving upon OTR's pricing models.

17. On November 2, 2018, DI and OTR signed a non-disclosure confidentiality agreement ("NDA") related to OTR's confidential and proprietary information, as defined in the NDA, which Data Interfuse may receive, have access to, or use of in the event OTR agreed to hire DI as an IT consultant. (A copy of the NDA is attached as **Exhibit A**).

18. The NDA provides that "Confidential Material will be kept confidential by the Receiving Party" and that the Receiving Party agrees that it and its Representatives will not use, apply, disclose or otherwise make available any Confidential Material that is accorded 'trade secret' status under any applicable law". (See Exhibit A at p. 1-2).

19. DI agreed to assist OTR to develop and improve a pricing model platform for OTR to use in its business. During the ensuing year, OTR and Data Interfuse negotiated the terms of the agreement and discussed the scope of the work that needed to be performed. OTR provided "Confidential Material" to Data Interfuse in connection with negotiating the terms of the agreement.

20. On November 22, 2019, DI and OTR entered a Master Services Agreement ("Agreement") that established the duties and obligations related to DI's technology, coding, consultant and engineering services for OTR. (A copy of the Agreement is attached as **Exhibit B**).

21. Section 3.2 of the Agreement incorporates the NDA by reference and provides for rights and duties of OTR and DI with respect to each other's "Confidential Information" and use of "Confidential Material". (See Exhibit B § 3.2 at p. 4).

22. DI agreed to serve as an independent contractor consultant of OTR under the Agreement. (See Exhibit B § 7.2 at p. 7-8).

23. Following execution of the Agreement, OTR continued to provide Confidential Information and Confidential Material to DI in connection with the scope of the Services, Deliverables, Work, and Work Product (each as defined in the Agreement) that DI provided to OTR while performing under the Agreement.

24. OTR's Confidential Information and Confidential Material provided to DI under the Agreement included, but was not limited to, proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data and information that OTR keeps confidential and secret from third parties and from which OTR derives economic value because such data and information is and remains confidential and not disclosed or known to the public.

25. All Deliverables and Work Product created by DI on behalf of OTR are the rightful and lawful property of OTR under the Agreement.

26. Section 2.1 of the Agreement provides:

> Ownership and License Rights. The Work Product has been specially ordered and commissioned by Company. Consultant agrees that the Work Product is a "work made for hire," as that term is defined in the United States Copyright Act, with all copyrights in the Work owned solely by Company. To the extent that the Work Product does not qualify as a work made for hire under applicable law, and to the extent that the Work Product includes material subject to copyright, patent, trade secret, or other proprietary right protection, Consultant hereby assigns to Company all right, title and interest in and to the Work Product; including all rights in and to any inventions and designs embodied in the Work Product that are developed within the narrowly-defined scope of the engagement during the course of

> Consultant's creation of the Work Product. For the avoidance of doubt, Company will have the right to use, and authorize or license third parties to use, the Work Product in any and all matter and media and in all channels of distribution (whether now known or hereafter devised) throughout the world in perpetuity without further obligation to Consultant. To the maximum extent permitted by law, Consultant waives all moral rights in the Work. Notwithstanding these assignments relative to granular Work Product, Company understands and agrees that, in the course of preparing written or verbal reports, studies, analyses, research data, proposals, strategies, or similar Work Product under this agreement, Consultant may leverage certain proprietary methodologies, best practices, frameworks, visualization tools, and other repurposable methods (collectively, "Methods"). Company shall be granted a perpetual non-transferable, non-exclusive license to use, re-use, repurpose, and distribute INTERNAL TO COMPANY ONLY the underlying Methods used to derive these Work Products, but, except insofar as Company may already have developed and used these same Methods prior to engagement of Consultant, rights to these Methods may not be transferred by Company to any third party without Consultant's prior written approval.

(Exhibit B § 2.1 at p.3).

27. In order for DI to efficiently work on OTR's requested deliverables, OTR granted DI access to OTR's database by setting up specific DI accounts within OTR's database hosted by Amazon Web Services ("AWS"). These accounts were: abernier[@]datainterfuse.com; dtran[@]datainterfuse.com; ttran[@]datainterfuse.com; jlovegrove[@]datainterfuse.com; and tjohnston[@]datainterfuse.com.

28. DI would use these accounts to access OTR information during the course of the parties' engagement.

29. In and around September of 2020, OTR expressed its dissatisfaction with DI's quality of deliverables, and more specifically the lack thereof, and DI conceded that a new team of DI employees would be needed to work on OTR's deliverables to create and develop a price modelling platform in accordance with the Agreement and the expectations of OTR.

30. At that time, DI and OTR discussed DI's future role in assisting OTR build out a proprietary software program that had the potential to be very valuable and capable of being used by, or sold to, not only the transportation industry but in a wide variety of different industries.

31. At the time of these September 2020 conversations, the Agreement between OTR and DI was set to expire by its terms in approximately two (2) months.

32. The express terms of the Agreement provide that the Agreement will terminate after a twelve (12) month period unless renewed by the parties or terminated early in accordance with its terms. (See Exhibit B § 5.1 at p. 5).

33. In the beginning of November 2020, DI proposed entering into a new agreement with OTR, the terms of which were drastically different than the existing Agreement.

34. Specifically, the proposed new agreement would grant DI a license to use and exploit for its own gain the deliverables DI created for OTR. As such, OTR rejected the proposed new agreement, and OTR and DI did not negotiate further or enter into any subsequent contract.

35. At that time, OTR had concerns that DI had intentions of exploiting and taking ownership of the proprietary software OTR was planning to build, which OTR and DI discussed in September 2020.

36. As such, the Agreement between DI and OTR terminated by its terms on November 22, 2020 – twelve (12) months following execution by DI's duly authorized officer. (See Exhibit B § 5.1 at p. 5 and 11).

37. Upon termination of the Agreement, DI was to return all Confidential Information in its possession, custody, or control to OTR upon request.

38. Section 5.4 of the Agreement provides:

> Return of Information. Upon termination of this Agreement for any reason, Consultant shall, upon request by Company, immediately return to Company all Confidential Information which is within Consultant's possession or control.

(Exhibit B § 5.4 at p. 6).

39. On November 24, 2020, OTR advised DI that the Agreement would be not be renewed or extended ("Notice of Termination Date"), the Services provided by DI for the work and deliverables would no longer be necessary and that the consulting relationship in its entirety was terminated.

40. DI acknowledged OTR's termination of the Agreement via email the following day. (A copy of the November 25, 2020 email is attached as **Exhibit C)**.

41. In the November 25, 2020 acknowledgement email, Jimmy Fernandes, DI's President, represented to OTR that: "As we discussed, Data Interfuse is not interested in holding ANY of your proprietary information. That was never the intent. John Lovegrove will discuss the transfer of any information as you direct." (See Exhibit C at p. 1).

42. After sending the November 25, 2020 email, DI did not return OTR's proprietary information, including OTR's Confidential Information and Confidential Material in the possession, custody, and control of Data Interfuse nor otherwise disclose any portals of other on-ramps into OTR's proprietary AWS account.

43. On December 8, 2020, OTR transmitted a letter via email to DI demanding that DI return OTR's property and Confidential Information with respect to the Work and Deliverables still in Data Interfuse's possession, custody, and control. (A copy of the December 8, 2020 demand letter is attached as **Exhibit D**).

44. DI never returned any information or property whatsoever to OTR.

45. At no point did OTR intend to give DI unfettered access to its information.

46. OTR used reasonable methods to keep its information secure and protected.

47. On December 8, 2020, OTR became aware that DI accounts were still linked to OTR's proprietary AWS database. OTR immediately attempted to remove DI's access to OTR's database and disabled DI's accounts that were known to OTR.

48. In and around February 2021, OTR had suspicions that the security system for its database and software program were breached.

49. On February 23, 2021, OTR became aware of unauthorized peering sessions into their database hosted by Amazon ("AWS account"). These sessions were discovered to have been setup by an unauthorized account associated with the Gmail account "johnlovegrove1957[@]gmail.com."

50. Defendants DI and Lovegrove used the peering sessions to access OTR's proprietary electronic data system and otherwise monitor, copy and acquire portions or all of OTR's proprietary pricing modeling system and other pricing data.

51. At no time did OTR give DI or Lovegrove approval to create an account under Lovegrove's Gmail account. Lovegrove already had an account which used his DI email address; therefore, there was no need for him to create a separate account using his personal Google Gmail address.

52. OTR attempted to close the connections and shut off Lovegrove's access to OTR's data soon after the Gmail account was discovered.

53. When OTR closed the connections to the Lovegrove Gmail account, it became immediately apparent that OTR's operational database was compromised and OTR's proprietary software program had been rendered inoperable.

54. OTR employees worked around the clock to repair OTR's database and software system.

55. During this time, OTR's operations were halted and OTR was unable to efficiently close its transactions and otherwise operate its business for approximately twenty-four (24) hours.

56. OTR then hired a tech forensic expert to investigate the cause of the problem that shut down OTR's software program.

57. OTR's forensic expert discovered that the unauthorized "johnlovegrove1957[@]gmail.com" account was set up on OTR's database sometime before September 30, 2020.

58. On or about September 30, 2020, the unauthorized Lovegrove Gmail account was granted role permissions to the root account within OTR's AWS database, which allowed the Lovegrove Gmail account to assume any role within the database. Stated differently, the unauthorized Lovegrove Gmail account's functions and permissions were manipulated such that the Lovegrove Gmail account could perform functions in OTR's database under the guise of another authorized OTR account.

59. Upon information and belief, the unauthorized Lovegrove Gmail account reinstated the jlovegrove[@]datainterfuse.com account shortly after it was disabled on December 8, 2020.

60. OTR's expert concluded that between November 30, 2020 and January 2, 2021, there were 160 instances whereby the jlovegrove[@]datainterfuse.com account performed the action "DescribeEventAggregates" which allowed the user of the account to access and view OTR's operations, including the status of the proprietary software OTR was building.

61. OTR's expert also discovered that a "logic bomb" was planted in OTR's system.

62. A logic bomb is commonly described in the tech industry as "a type of malware that executes a set of instructions to compromise information systems…Logic bombs are usually programs that use either time or an event as the trigger. When the condition(s) stipulated in the instruction set is met, the code present in its payload is executed. It is mostly used by disgruntled employees planning revenge on their employers or by Blackhat hackers for financial gains." DOJML Title 9-7811§ [9-48.000D] CYBER-INVESTIGATIVE ISSUES II, DOJML COMMENT 9-48.000D.

63. OTR learned that when the logic bomb was triggered on February 23, 2021, it caused OTR's software to engage in a perpetual loop, thereby making it impossible for OTR's system to run properly. OTR's expert found that this logic bomb was specifically coded so that it would trigger in the event OTR cut the connection between OTR's database and the unauthorized Lovegrove Gmail account.

64. OTR's expert concluded that after November 22, 2020, DI and Lovegrove, through various DI accounts and the Lovegrove Gmail account, obtained unauthorized access to OTR's database, reviewed proprietary information, deleted OTR information, changed passwords, deleted login profiles, manipulated account groups, reviewed details about user profiles and status upgrades, and otherwise manipulated, interfered with and destroyed OTR data.

65. At no point after November 22, 2020 did OTR give DI authority to access, copy or acquire its pricing and other database, software program or other pricing information.

66. Upon information and belief, DI and Lovegrove accessed DI's database and software system for purposes of monitoring and stealing OTR's proprietary software.

COUNT I
VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT
18 U.S.C. § 1030

67. OTR hereby incorporates by reference Paragraphs 1 through 66 above in this First Count as though fully set forth herein.

68. DI and Lovegrove knowingly and intentionally gained unauthorized access to OTR's computer system with the intent to defraud. OTR's computer system consists of its computers, the associated software, its servers, its database, and all documents and information stored on the system (the "Computer System").

69. OTR did not authorize DI or Lovegrove individually to access its Computer System after the Agreement was terminated on November 22, 2020.

70. DI and Lovegrove fraudulently gained access to OTR's Computer System by creating and planting the Lovegrove Gmail account within OTR's Computer System at a time when OTR had no reason to question DI's presence in OTR's Computer System. DI and Lovegrove planted this account and concealed its existence with the intention of later using that account to gain unauthorized access to OTR's Computer System in the event DI's access was disabled.

71. By gaining access to OTR's Computer System, DI and Lovegrove obtained access to OTR's computers, servers, all associated software, its database and all documents and information stored on the system, all of which are routinely used in and affect interstate commerce, as OTR uses these systems on a daily basis in its multi-state transportation logistics business.

72. OTR's Computer System constitutes protected computers under 18 U.S.C. § 1030.

73. DI and Lovegrove gained unauthorized access, and exceeded their authorized access, to OTR's Computer System.

74. In gaining unauthorized access and otherwise exceeding their authorized access, DI and Lovegrove obtained valuable proprietary information belonging exclusively to OTR, and also knowingly and intentionally inflicted damage and loss to OTR's Computer System. The damage consisted of technological harms, such as impairing the integrity of OTR's Computer System, and making programs, data and the entire system unavailable to OTR for the conduct of its business. The loss consisted of the loss of computer data, computer programs, and information services.

75. OTR has incurred costs in the approximate amount of $70,000 to restore and protect its Computer System, to disable DI and Lovegrove's unauthorized access, and to investigate the cause of the Computer System shutdown and the extent of DI and Lovegrove's misconduct.

76. Furthermore, as a result of the trigger of the logic bomb, OTR lost approximately two full work-days of operational control over its Computer System, which prohibited it from initiating new freight brokerage agreements, updating its clients on existing brokerage agreements, and otherwise prohibiting it from doing business in any respect.

77. Defendants DI and Lovegrove intentionally set up a network of unauthorized peering sessions, portals and other backdoor access points to intentionally access and acquire without authorization OTR's proprietary electronic data system and otherwise monitor, copy and acquire portions or all of OTR's proprietary company information, pricing modeling system and other pricing and transportation data.

78. At the same time, DI and Lovegrove used the unauthorized peering sessions and/or backdoor access points to install one or more logic bombs into OTR's system that would make it difficult to trace and otherwise determine the source of the meltdown of OTR's company electronic data system without extensive and expensive outside expert forensic analysis.

79. DI and Lovegrove's actions in planting the logic bomb was intentional, malicious willful and wanton and was intended to inflict maximum damage to OTR's daily operations.

80. DI and Lovegrove had unfettered unauthorized access to OTR's entire customer database, proprietary pricing information, development stage price modeling system and other vital and proprietary company electronic data, and otherwise improperly acquired some or all of OTR's proprietary data.

81. DI and Lovegrove intentionally caused proprietary OTR data, specifically computer code relating to the developmental stage pricing model that DI had been working on, to be transmitted to Defendants from OTR's protected AWS account. Defendant's unauthorized acquisition of OTR's proprietary electronic data and damage thereto is in violation of 18 U.S.C. 1030(a)(4) and (5).

82. DI and Lovegrove's unauthorized access to OTR's proprietary company electronic data occurred after the termination of the DI/OTR Agreement and was specifically prohibited under the terms of the written Non-disclosure Confidentiality Agreement.

83. OTR was damaged in that proprietary customer data, pricing information and computer code relating to its development stage price modeling system and other vital and proprietary company electronic data was comprised and otherwise acquired by Defendants.

84. OTR was further damaged in that the logic bomb installed by Defendant into OTR's system shut down OTR's entire company operations for approximately twenty-four hours, and OTR was required to retain expert forensic computer consultants to first repair its computer system, and then conduct a forensic analysis to uncover the unauthorized back-door access points installed by Defendants and to track and identify the logic bomb as the cause of the shutdown of the company computer system.

85. Defendants' planting of the logic bomb was an intentional, willful and wanton act whereby Defendants knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer in violation of 18 USC 1020(a)(5)(A).

WHEREFORE, Plaintiff OTR Transportation, Inc. respectfully requests that this Court enter a judgment in its favor and against John Lovegrove and Data Interfuse, LLC for violation of 18 U.S.C. §1030(a)(2)(c); 1030(a)(4), 1030(a)(5)(A), and pursuant to 18 U.S.C. §1030(g) enter the following relief:

a) Compensatory damages in an amount to be proven at trial in excess of $75,000 for Defendants' unauthorized acquisition of OTR's proprietary electronic data in violation of 18 U.S.C. 1030(a)(4);

b) Compensatory damages in an amount to be proven at trial in excess of $75,000 for Defendants knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer in violation of 18 USC 1020(a)(5)(A)

c) A preliminary and permanent injunction prohibiting Defendants John Lovegrove and Data Interfuse, LLC from accessing or otherwise interfering with the Computer Systems of Plaintiff OTR Transportation, Inc.;

d) A preliminary and permanent injunction requiring the deletion of OTR Transportation Inc.'s information and data in the possession of Defendants John Lovegrove and/or Data Interfuse, LLC;

e) A preliminary and permanent injunction prohibiting Defendants John Lovegrove and Data Interfuse, LLC from using, transmitting, or otherwise utilizing OTR Transportation Inc.'s Computer Systems, data and information;

f) All attorneys' fees and costs in pursuing this action; and

g) All such other and further relief as is deemed appropriate under the terms of 18 U.S.C. 1030 et seq. or the equitable authority of this Court.

COUNT II
VIOLATION OF ILLINOIS TRADE SECRETS ACT
765 ILCS 1065

1-66. Plaintiffs repeat and reallege paragraphs 1-66 of the allegations common to all counts as paragraphs 1-66 of this Count II.

67-85. Plaintiffs further repeat and reallege paragraphs 67-85 of Count I of Plaintiff's Complaint as allegations 67 to 84 of this Count II.

86. The Illinois Trade Secret Act defines a Trade Secret as:

> information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that:
>
> (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
>
> (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

765 Ill. Comp. Stat. Ann. 1065/2

87. On November 22, 2018, OTR entered into a Non-Disclosure Confidentiality Agreement with DI whereby Defendant DI agreed to treat all OTR's proprietary electronic data as confidential as follows:

> Confidential Material will be kept confidential by the "Receiving Party" and that the Receiving Party agrees that it and its Representatives will not use, apply, disclose or otherwise make available any Confidential Material that is accorded 'trade secret' status under any applicable law.

(See Exhibit A).

88. Thereafter on November 22, 2020, OTR and DI entered into a Data Interfuse Master Service Agreement. (See Exhibit B). In that Agreement, OTR and DI outlined the confidentiality Obligations as follows:

> Consultant may have executed Company's Mutual Nondisclosure Agreement ("NDA") prior to or at the time of execution of this Agreement, or may be asked to do so in the future. Where this NDA has been executed, its terms are incorporated herein by reference. If no NDA has been executed, Consultant and Company shall (a) hold the Confidential Information of the other in confidence and protect the same with at least the same degree of care, but no less than reasonable care, with which it protects its own most sensitive confidential information, and (b) use the Confidential Information of the other solely in connection with the exercise of its rights and the performance of its obligations under this Agreement. As used herein, the term "Confidential Information" means any data, materials, documents or information disclosed by either party to the other either during or in connection with this Agreement that is not generally known to the public, and is clearly identified as confidential or, by its nature, should be reasonably considered confidential.

Id.

89. DI operated as one of OTR's technology consultants from November 22, 2019 until it was terminated by operation of the Agreement on November 22, 2020. During that period, DI disclosed certain proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data and information that OTR keeps confidential and secret from third parties and from which OTR derives economic value because such data and information is and remains confidential and not disclosed or known to the public.

90. During that same one-year period, DI focused much of its attention on helping to develop OTR's proprietary pricing modeling system using pricing data from OTR and other proprietary OTR data sources.

91. Unlike many consulting agreements, OTR's Agreement with DI mandated that All Deliverables and Work Product created by DI on behalf of OTR are the rightful and lawful property of OTR under the Agreement. (Exhibit B § 2.1).

92. In addition to executing confidentiality agreements with its vendors such as DI, OTR also required all its sales and necessary support staff to execute confidentiality agreements similar to the one signed by DI in order to protect the integrity of OTR's pricing and other proprietary data.

93. All such efforts by OTR to maintain the secrecy of its proprietary electronic and other information are the subject of efforts that are reasonable under the circumstances to maintain the secrecy of OTR's proprietary and confidential trade secrets.

94. OTR routinely restrained or restricted access to its proprietary customer ordering and pricing information, as well as to its pricing modeling software, and limited access to such information using password-protected systems and limiting access to such data to a limited number of OTR officers and employees on a need to know basis, and implemented other tools and mechanisms to maintain the secrecy of its proprietary customer and pricing data.

95. Days after OTR terminated the DI Agreement, Jimmy Fernandes, DI's President, represented to OTR that, "As we discussed, Data Interfuse is not interested in holding ANY of your proprietary information. That was never the intent. John Lovegrove will discuss the transfer of any information as you direct." (See Exhibit C at p. 1).

96. After sending the November 25, 2020 email, DI did not return OTR's proprietary information, including OTR's Confidential Information and Confidential Material in the possession, custody, and control of Data Interfuse nor otherwise disclosed any portals of other on-ramps into OTR's proprietary AWS account.

97. On December 8, 2020, OTR sent a letter via email to DI demanding that DI return OTR's property and Confidential Information with respect to the Work and Deliverables still in Data Interfuse's possession, custody, and control. (See Exhibit D).

98. DI currently retains possession of certain OTR proprietary and confidential information and has refused to return such information despite repeated demands from OTR to return such information.

99. Information that has been improperly retained by DI following the termination of the Agreement includes proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data and information that OTR keeps confidential and secret from third parties and from which OTR derives economic value because such data and information is and remains confidential and not disclosed or known to the public.

100. The OTR information improperly retained by DI is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use.

101. Months after the termination of the OTR/DI Agreement on February 23, 2021, OTR became aware of unauthorized peering sessions into their database hosted by Amazon ("AWS Account"). These sessions were discovered to have been set up by an unauthorized account associated with the Gmail account "johnlovegrove1957[@]gmail.com."

102. As a result, OTR retained an electronic data forensic expert that determined that between November 30, 2020 and January 2, 2021, there were 160 instances whereby the jlovegrove[@]datainterfuse.com account performed the action "DescribeEventAggregates" which allowed the user of the account to review OTR operations, including the status of the proprietary software OTR was building.

103. DI and Lovegrove's unauthorized access to OTR's proprietary company electronic data occurred after the termination of the DI/OTR Agreement and was specifically prohibited under the terms of the written Non-Disclosure Confidentiality Agreement.

104. OTR has been damaged in that its confidential and proprietary trade secrets have been improperly retained by Defendant DI after termination of the Agreement, despite repeated written demands by OTR for the return of such information.

105. DI and Lovegrove's unauthorized access to OTR's proprietary company electronic data occurred after the termination of the DI/ORT Agreement, and was specifically prohibited under the terms of the written Non-Disclosure Confidentiality Agreement.

106. OTR was damaged in that proprietary customer data, pricing information and computer code relating to its development stage price modeling system and other vital and proprietary company electronic data was comprised and otherwise acquired by Defendants.

107. In an apparent retaliation for the termination of the DI/OTR Agreement and the repeated demand for the return of the trade secret information, Defendants -- using illegally created back doors to the OTR system -- installed a logic bomb that immediately shut down OTR's entire company electronic database, thereby halting OTR's operations for approximately twenty-four (24) hours.

108. Defendants' planting of the logic bomb was an intentional, willful and wanton act that was initiated after Plaintiff allowed the OTR/DI Agreement to expire, and after Plaintiff thereafter lawfully demanded the return of its trade secret information.

109. Defendants have sustained damage as a result of Defendants' blatant refusal to return OTR's proprietary trade secret information including, but not limited to, proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data in that such data is currently being held by DI without authorization.

WHEREFORE, Plaintiff OTR Transportation, Inc. respectfully requests that this Court enter a judgment in its favor and against John Lovegrove and Data Interfuse, LLC for violation of the Illinois Trade Secret Act as follows:

a) Compensatory damages in an amount to be proven at trial in excess of $75,000 for Defendants' violation of the Illinois Trade Secrets Act;

b) Compensatory damages in an amount not exceeding twice any award made pursuant to the Illinois Trade Secret Act;

c) A preliminary and permanent injunction requiring the deletion of OTR Transportation Inc.'s information and data in the possession of Defendants John Lovegrove and/or Data Interfuse, LLC;

d) A preliminary and permanent injunction prohibiting Defendants John Lovegrove and Data Interfuse, LLC from using, transmitting, or otherwise utilizing Plaintiff OTR Transportation Inc.'s Computer Systems, data and information;

e) All attorneys' fees and costs in pursuing this action;

f) Any and all punitive damages as allowed under Illinois law; and

g) Any other relief this Court deems equitable under the circumstances.

COUNT III
VIOLATIONS OF THE DEFEND TRADE SECRETS ACT (DTSA)
18 U.S.C.A. § 1839, et al.

1-66. Plaintiffs repeat and reallege paragraphs 1-66 of the allegations common to all counts as paragraphs 1-66 of this Count III.

67-85. Plaintiffs further repeat and reallege paragraphs 67-85 of Count I of Plaintiff's Complaint as allegations 67 to 85 of this Count III.

110. The Defend Trade Secret Act defines a Trade Secret as:

> forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

18 U.S.C.A. § 1839.

111. On November 22, 2018, OTR entered into a Non-Disclosure Confidentiality Agreement with DI whereby Defendant DI agreed to treat all OTR's proprietary electronic data as confidential as follows:

> Confidential Material will be kept confidential by the "Receiving Party" and that the Receiving Party agrees that it and its Representatives will not use, apply, disclose or otherwise make available any Confidential Material that is accorded 'trade secret' status under any applicable law.

(See Exhibit A).

112. Thereafter on November 22, 2020, OTR and DI entered into a Data Interfuse Master Service Agreement. (See Exhibit B). In that Agreement, OTR and DI outlined the confidentiality Obligations as follows:

> Consultant may have executed Company's Mutual Nondisclosure Agreement ("NDA") prior to or at the time of execution of this Agreement, or may be asked to do so in the future. Where this NDA has been executed, its terms are incorporated herein by reference. If no NDA has been executed, Consultant and Company shall (a) hold the Confidential Information of the other in confidence and protect the same with at least the same degree of care, but no less than reasonable care, with which it protects its own most sensitive confidential information, and (b) use the Confidential Information of the other solely in connection with the exercise of its rights and the performance of its obligations under this Agreement. As used herein, the term "Confidential Information" means any data, materials, documents or information disclosed by either party to the other either during or in connection with this Agreement that is not generally known to the public, and is clearly identified as confidential or, by its nature, should be reasonably considered confidential.

Id.

113. DI operated as one of OTR's technology consultants from November 22, 2019 until it was terminated by operation of the Agreement on November 22, 2020. During that period, DI disclosed certain proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data and information that OTR keeps confidential and secret from third parties and from which OTR derives economic value because such data and information is and remains confidential and not disclosed or known to the public.

114. During that same one-year period, DI focused much of its attention on helping to develop OTR's proprietary pricing modeling system using pricing data from OTR and other proprietary OTR data sources.

115. Unlike many consulting agreements, OTR's Agreement with DI mandated that All Deliverables and Work Product created by DI on behalf of OTR are the rightful and lawful property of OTR under the Agreement. (Exhibit B § 2.1).

116. In addition to executing confidentiality agreements with its vendors such as DI, OTR also required all its sales and necessary support staff to execute confidentiality agreements similar to the one signed by DI in order to protect the integrity of OTR's pricing and other proprietary data.

117. All such efforts by OTR to maintain the secrecy of its proprietary electronic and other information are the subject of efforts that are reasonable under the circumstances to maintain the secrecy of OTR's proprietary and confidential trade secrets.

118. OTR routinely restrained or restricted? access to its proprietary customer ordering and pricing information as well as to its pricing modeling software and limited access to such information using password-protected systems and limiting access to such data to a limited number of OTR officers and employees on a need to know basis and implemented other tools and mechanisms to maintain the secrecy of its proprietary customer and pricing data.

119. Days after OTR terminated the DI Agreement, Jimmy Fernandes, DI's President, represented to OTR that, "As we discussed, Data Interfuse is not interested in holding ANY of your proprietary information. That was never the intent. John Lovegrove will discuss the transfer of any information as you direct." (See Exhibit C at p. 1).

120. After sending the November 25, 2020 email, DI did not return OTR's proprietary information, including OTR's Confidential Information and Confidential Material in the possession, custody, and control of Data Interfuse nor otherwise disclosed any portals of other on-ramps into OTR's proprietary AWS account.

121. On December 8, 2020, OTR sent a letter [via email] to DI demanding that DI return OTR's property and Confidential Information with respect to the Work and Deliverables still in Data Interfuse's possession, custody, and control. (See Exhibit D).

122. DI currently retains possession of certain OTR proprietary and confidential information and has refused to return such information despite repeated demands from OTR to return such information.

123. Information that has been improperly retained by DI following the termination of the Agreements includes proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data and information that OTR keeps confidential and secret from third parties and from which OTR derives economic value because such data and information is and remains confidential and not disclosed or known to the public.

124. The OTR information improperly retained by DI is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use.

125. Months after the termination of the OTR/DI Agreement on February 23, 2021, OTR became aware of unauthorized peering sessions into their database hosted by Amazon ("AWS Account"). These sessions were discovered to have been set up by an unauthorized account associated with the Gmail account "johnlovegrove1957[@]gmail.com."

126. As a result, OTR retained an electronic data forensic expert that determined that between November 30, 2020 and January 2, 2021, there were 160 instances whereby the jlovegrove[@]datainterfuse.com account performed the action "DescribeEventAggregates" which allowed the user of the account to review OTR operations, including the status of the proprietary software OTR was building.

127. DI and Lovegrove's unauthorized access to OTR's proprietary company electronic data occurred after the termination of the DI/OTR Agreement and was specifically prohibited under the terms of the written Non-Disclosure Confidentiality Agreement.

128. OTR has been damaged in that its confidential and proprietary trade secrets have been improperly retained by Defendant DI despite repeated written demands by OTR for the return of such information.

129. DI and Lovegrove's unauthorized access to OTR's proprietary company electronic data occurred after the termination of the DI/ORT Agreement and was specifically prohibited under the terms of the written Non-Disclosure Confidentiality Agreement.

130. OTR was damaged in that proprietary customer data, pricing information and computer code relating to its development stage price modeling system and other vital and proprietary company electronic data was comprised and otherwise acquired by Defendants.

131. In an apparent retaliation for the termination of the DI/OTR agreement and the repeated demand for the return of the trade secret information, Defendants -- using illegally created

back doors to the OTR system -- installed a logic bomb that immediately shut down OTR's entire company electronic database thereby halting OTR's operations for approximately twenty-four (24) hours.

132. Defendants' planting of the logic bomb was an intentional, willful and wanton act that was initiated after Plaintiff allowed the OTR/DI Agreement to expire and thereafter lawfully demanded the return of its trade secret information.

133. Defendants have sustained damage as a result of Defendants' blatant refusal to return OTR's proprietary trade secret information including, but not limited to, proprietary pricing data, customer pricing data, customer data, customer lists, price modeling data, customer load history data, carrier pricing data, customer data bases, material, documents, electronic files, business information, financial records, proprietary business records, financial data, formulas, compilations, technical data, non-technical data, programs, methods, techniques, processes, customer lists, prospective customer lists, and other data in that such data is currently being held by DI without authorization.

WHEREFORE, Plaintiff OTR Transportation, Inc. respectfully requests that this Court enter a judgment in its favor and against John Lovegrove and Data Interfuse, LLC for violation of the Defend Trade Secret Act as follows:

a) Compensatory damages in an amount to be proven at trial in excess of $75,000 for Defendants' violation of the Illinois Trade Secrets Act;

b) Compensatory damages pursuant to the Defend Trade Secret Act;

c) A preliminary and permanent injunction requiring the deletion of OTR Transportation Inc.'s information and data in the possession of Defendants John Lovegrove and/or Data Interfuse, LLC;

d) A preliminary and permanent injunction prohibiting Defendants John Lovegrove and Data Interfuse, LLC from using, transmitting, or otherwise utilizing Plaintiff OTR Transportation Inc.'s Computer Systems, data and information;

e) All attorneys' fees and costs in pursuing this action;

f) Any and all punitive damages as allowed under Illinois law; and

g) Any other relief this Court deems equitable under the circumstances.

COUNT IV
INTENTIONAL INTERFERENCE WITH CONTRACTUAL RELATIONS

1-66. Plaintiffs repeat and reallege paragraphs 1-66 of the allegations common to all counts as paragraphs 1-66 of this Count IV.

67-85. Plaintiffs further repeat and reallege paragraphs 67-85 of Count I of Plaintiff's Complaint as allegations 67 to 85 of this Count IV.

86-108. Plaintiffs further repeat and reallege paragraphs 86-108 of Count II of Plaintiff's Complaint as allegations 86 to 108 of this Count IV.

134. OTR has active and ongoing contracts with its freight transportation carriers.

135. On February 23, 2021, when OTR's Computer System was down due to the logic bomb planted by DI and/or Lovegrove, nearly all of OTR's contracts with its freight transportation carriers were adversely affected, as OTR was not able to efficiently close its transactions and otherwise operate its business for approximately twenty-four (24) hours.

136. DI and Lovegrove both knew that OTR had these contractual business relationships with its freight transportation carriers, and they knew that if OTR's Computer System was down, OTR's business and revenue would be greatly affected.

137. DI and Lovegrove intentionally and unjustifiably interfered with OTR's ability to operate its business and carry out its obligations to its freight transportation carriers in accordance with its contractual relationships with its transportation carriers.

138. As a result of DI and Lovegrove's willful and malicious conduct, OTR was unable to close its transactions, monitor its freight, and otherwise provide brokerage services to its customers, which resulted in a total lost gross profit of approximately $22,000.00.

139. OTR also incurred expenses in the approximate amount of $70,000 to restore and protect its Computer System, to disable DI and Lovegrove's unauthorized access, and to investigate the cause of the Computer System shutdown and the extent of DI and Lovegrove's misconduct.

WHEREFORE, Plaintiff OTR Transportation, Inc. respectfully requests that this Court enter a judgment in its favor and against John Lovegrove and Data Interfuse, LLC as follows:

a) Compensatory damages in an amount to be proven at trial in excess of $75,000;

b) All attorneys' fees and costs in pursuing this action;

c) Punitive damages for defendants' intentional and malicious misconduct; and

d) Any other relief this Court deems equitable under the circumstances.

Respectfully submitted,

OTR Transportation, Inc.

By: Thomas P. Yardley, Jr.
One of its attorneys

Thomas P. Yardley, Jr. (ARDC No. 6208239
Christine R. Walsh (ARDC No. 6319177)
Robbins, Salomon & Patt, Ltd.
180 N. LaSalle Street
Suite 3300
Chicago, Illinois 60601
(312) 456-0184
tyardley@rsplaw.com
cwalsh@rsplaw.com